101665,484

3

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月１０日

出願番号
Application Number: 特願２００２－２９７８８８

[ST. 10/C]: [ＪＰ２００２－２９７８８８]

出願人
Applicant(s): 株式会社リコー

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７７３７

【書類名】　特許願

【整理番号】　0206950

【提出日】　平成14年10月10日

【あて先】　特許庁長官　太田　信一郎　殿

【国際特許分類】　G06F 12/00　537

【発明の名称】　セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置、ネットワーク配信を行う方法及び、セキュリティポリシーを外部から設定する入出力装置

【請求項の数】　76

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　斉藤　敦久

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　金井　洋一

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　谷内田　益義

【特許出願人】

【識別番号】　000006747

【氏名又は名称】　株式会社リコー

【代理人】

【識別番号】　100070150

【弁理士】

【氏名又は名称】　伊東　忠彦

【先の出願に基づく優先権主張】

【出願番号】　特願2002-275973

【出願日】　平成14年 9月20日

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9911477

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置、ネットワーク配信を行う方法及び、セキュリティポリシーを外部から設定する入出力装置

【特許請求の範囲】

【請求項１】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、

前記読み取り方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取る方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了するステップと、
を有する、セキュリティポリシーに基づいた文書の読み取り方法。

【請求項２】　前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項１に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項３】　前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項１あるいは２に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項４】　前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項３に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項５】　前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項１乃至４のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項６】　請求項１乃至５のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【請求項７】　請求項６に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項８】　請求項６に記載のプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置。

【請求項９】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、
少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、
読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、
前記組み合わせで読み取りを実行する場合の要件と、
を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、

前記読み取り装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、

を有する、セキュリティポリシーに基づいた文書の読み取り装置。

【請求項１０】　前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項９に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１１】　前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項９あるいは１０に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１２】　前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項

１１に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１３】　前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項９乃至１２のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項１４】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法であって、

前記文書を読み取り且つネットワーク配信を行う方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りとネットワーク配信が許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記文書の読み取りとネットワーク配信が許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には

、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りとネットワーク配信を行って終了するステップと、

を有するセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１５】　前記実行可能な要件が、前記読み取った文書データに電子透かしを埋め込むことである、請求項１４に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１６】　前記実行対応可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項１４あるいは１５に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１７】　前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項１５に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１８】　前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項１４乃至１７のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項１９】　前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項１４乃至１８のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項２０】　前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである、請求項１９に記載のセキュリティポリシーに基づいて文書を読み

取り且つネットワーク配信を行う方法。

【請求項２１】　前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項１４乃至２０のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項２２】　請求項１４乃至２１のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラム。

【請求項２３】　請求項２２に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項２４】　請求項２２に記載のプログラムをコンピュータにネットワーク配信するプログラム伝送装置。

【請求項２５】　少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づ

いて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、

を有する、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項２６】　前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項２５に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項２７】　前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項２５あるいは２６に記載のセキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う装置。

【請求項２８】　前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項２７に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項２９】　前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を

行うことである、請求項２５乃至２８のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項３０】　前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項２５乃至２９のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項３１】　前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである、請求項３０に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項３２】　前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項２５乃至３１のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項３３】　ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作する入出力装置において、前記ドキュメントセキュリティポリシーを外部から設定することを特徴とする入出力装置。

【請求項３４】　前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする、請求項３３記載の入出力装置。

【請求項３５】　設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とする、請求項３３或は３４に記載の入出力装置。

【請求項３６】　設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とする、請求項３３乃至３５に記載の入出力装置。

【請求項３７】　外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とする、請求項３３乃至３６に記載の入出力装置。

【請求項３８】　前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項３７に記載の入出力装置。

【請求項３９】　前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項３７或は３８に記載の入出力装置。

【請求項４０】　前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に、前記入出力装置自身の認証情報を送信することを特徴とする、請求項３９に記載の入出力装置。

【請求項４１】　前記外部のサーバへポリシー送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とする、請求項３９或は４０に記載の入出力装置。

【請求項４２】　前記入出力装置の電源が投入されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項３９或は４０に記載の入出力装置。

【請求項４３】　前記入出力装置内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項３９或は４０に記載の入出力装置。

【請求項４４】　前記入出力装置を操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項３９或は４０に記載の入出力装置。

【請求項４５】　取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とする、請求項３３乃至３６に記載の入出力装置。

【請求項４６】　前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記

ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とする、請求項４５に記載の入出力装置。

【請求項４７】　前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項４６記載の入出力装置。

【請求項４８】　前記入出力装置は、プリンタ、プリンタサーバ、スキャナ、スキャナサーバ、コピア、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とする、請求項３３乃至４７記載の入出力装置。

【請求項４９】　ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作するドキュメント処理ソフトウェアにおいて、前記前記ドキュメントセキュリティポリシーを外部から設定することを特徴とするドキュメント処理ソフトウェア。

【請求項５０】　ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする、請求項４９記載のドキュメント処理ソフトウェア。

【請求項５１】　設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とする、請求項４９或は５０に記載のドキュメント処理ソフトウェア。

【請求項５２】　設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とする、請求項４９乃至５１に記載のドキュメント処理ソフトウェア。

【請求項５３】　外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とする、請求項４９乃至５２に記載のドキュメント処理ソフ

トウェア。

【請求項５４】　前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項５３に記載のドキュメント処理ソフトウェア。

【請求項５５】　前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項５３或は５４に記載のドキュメント処理ソフトウェア。

【請求項５６】　前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に,前記ドキュメント処理ソフトウェア自身の認証情報を送信することを特徴とする、請求項５５に記載のドキュメント処理ソフトウェア。

【請求項５７】　前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とする、請求項５５或は５６に記載のドキュメント処理ソフトウェア。

【請求項５８】　前記ドキュメント処理ソフトウェアが起動されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項５５或は５６に記載のドキュメント処理ソフトウェア。

【請求項５９】　前記ドキュメント処理ソフトウェアの内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項５５或は５６に記載のドキュメント処理ソフトウェア。

【請求項６０】　前記ドキュメント処理ソフトウェアを操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項５５或は５６に記載のドキュメント処理ソフトウェア。

【請求項６１】　取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とする、請求項４９乃至５２に記載のドキュメント処理ソフトウェア。

【請求項６２】　前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とする、請求項６１に記載のドキュメント処理ソフトウェア。

【請求項６３】　前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項６２に記載のドキュメント処理ソフトウェア。

【請求項６４】　前記ソフトウェアは、プラグインであることを特徴とする、請求項４９乃至６３に記載のドキュメント処理ソフトウェア。

【請求項６５】　少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバと入出力装置からなるドキュメントシステムにおいて、前記入出力装置が前記サーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステム。

【請求項６６】　前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止或は許可する場合の要件が記述されていることを特徴とする、請求項６５に記載のドキュメントシステム。

【請求項６７】　前記入出力装置が前記サーバに対して、少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記入出力装置に対して、少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とする、請求項６５或は６６に記載のドキュメントシステム。

【請求項６８】　前記入出力装置が前記サーバに対して情報を送信する前に、前記入出力装置自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とする、請求項６７に記載のドキュメントシステム。

【請求項６９】　前記サーバが前記入出力装置に情報を送信する前に，前記サーバ自身の認証情報を送信し、前記入出力装置は受信した前記認証情報の検証を行うことを特徴とする、請求項６７或は６８記載のドキュメントシステム。

【請求項７０】　前記入出力装置は、プリンタ、プリンタサーバ、スキャナ、スキャナサーバ、コピア、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とする、請求項６５乃至６９に記載のドキュメントシステム。

【請求項７１】　少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバとドキュメント処理ソフトウェアからなるドキュメントシステムにおいて、 前記ドキュメント処理ソフトウェアがサーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステム。

【請求項７２】　前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする、請求項７１に記載のドキュメントシステム。

【請求項７３】　前記ドキュメント処理ソフトウェアが、前記サーバに対して少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記ドキュメント処理ソフトウェアに対して少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とする、請求項７１或は７２に記載のドキュメントシステム。

【請求項７４】　前記ドキュメント処理ソフトウェアが前記サーバに対して情報を送信する前に、前記ドキュメント処理ソフトウェア自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とする、請求項７３に記載のドキュメントシステム。

【請求項７５】　前記サーバが前記ドキュメント処理ソフトウェアに情報を送信する前に、前記サーバ自身の認証情報を送信し、前記ドキュメント処理ソフトウェアは、受信した前記認証情報の検証を行うことを特徴とする、請求項７３あるいは７４記載のドキュメントシステム。

【請求項７６】　前記ドキュメント処理ソフトウェアは、プラグインの形態をとることを特徴とする、請求項７１乃至７５に記載のドキュメントシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う方法、装置、プログラム、記憶媒体、伝送装置及び、セキュリティポリシーを外部から設定する入出力装置に関連する。

【０００２】

【従来の技術】

オフィスに代表されるような文書を扱うフィールドでは、その文書のセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等，特に情報のコンテナであるドキュメントに対するポリシー，中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。

【０００３】

現実に多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。

【０００４】

セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献１から、特許文献１４）。

【０００５】

例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献１）。

【０００６】

また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている(特許文献２)。

【０００７】

しかし、特に、上述の特許文献１では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。

【０００８】

また、上述の特許文献２では、セキュリティーポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるＤＢ（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。

【０００９】

また、特許文献７の操作者IDを入力させ、文書からIDを取り出し、複写を制御する方法では、複写を拒否する、又は、複写を許可してログを記録するという固定されたルールに基づく制御しか行えない。

【００１０】

特許文献８の画像から機密文書であることを示すマークを取り出してチェックする方法では、得られた情報からどのような動作を行うかまでが決められているため、ルールの柔軟性に欠ける。

【００１１】

特許文献９の印刷情報に含まれる出力制限データに基づいて出力先を制御する方法では、印刷情報にルールを含めなければならない。

【００１２】

特許文献１０の画像を読み取ってパスワードとともに記憶し,出力の際にパスワードが一致したときに許可する方法では、判断する基準がパスワードだけであり、それによって制御される動作も許可、又は、不許可だけである。

【００１３】

特許文献１１のネットワーク上の複数のMFPのうち、一つのMFPがユーザ管理を行ってネットワーク上のMFPすべての操作の許可、不許可を制御する方法では、制御される動作は許可、又は、不許可だけである。

【００１４】

特許文献１２の複数の機器について利用の許可、操作の許可をユーザごとに判断する方法では、許可,不許可だけしか制御できないし、ユーザ情報に基づいた制御しかできない。というように、従来技術の問題点はルールが限定的で柔軟性がなく、またそのルールもあらかじめ決められたものだけであるという欠点がある。すなわち、従来の入出力装置は、「ユーザ」と「ドキュメント」のIDに対する、操作の「許可」、「禁止」だけを、「あらかじめ」決められているものばかりである。

【００１５】

【特許文献１】

特開２００１－１８４２６４号公報

【特許文献２】

特開２００１－２７３３８８号公報

【特許文献３】

特開２００１－３３７８６４号公報

【特許文献４】

特開平０９－２９３０３６号公報

【特許文献５】

特開平０７－１４１２９６号公報

【特許文献６】

特許第０２７３５９６６号公報

【特許文献７】

特許３２０３１０３号公報

【特許文献８】

特開平７－５８９５０号公報

【特許文献９】

特開平７－１５２５２０号公報

【特許文献１０】

特開平１０－１９１０７２号公報

【特許文献１１】

特開２０００－１５８９８号公報

【特許文献１２】

特開２０００－３５７０６４号公報

【特許文献１３】

特開２００１－１２５７５９号公報

【特許文献１４】

特開２００１－３２５２４９号公報。

【００１６】

【発明が解決しようとする課題】

このようなセキュリティの設定方法では、文書印刷のセキュリティ設定をする場合には、第１に、設定者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第２には、すべての機器に対してセキュリティが、一つ一つ設定される必要がある。第３には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第４に、個々の機器にセキュリティ設定がされていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のようなの問題点がある。

本発明は、上述の問題点を解決することを目的とする。

【００１７】

特に本発明の目的は、文書に関するセキュリティポリシーに基づいて、紙文書

の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の読み取り装置を提供することである。

【００１８】

更に、本発明は、文書の読み取り装置や印刷装置等又は、その複合機において、今まで決められたルールに従った動作しかできなかったという課題を解決するために、外部からセキュリティポリシーを設定できる入出力装置を提供することである。

【００１９】

【課題を解決するための手段】

上記目的は、以下の本発明により解決される。

【００２０】

請求項１に記載の発明では、セキュリティポリシーに基づいた文書の読み取り方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、

前記読み取り方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキ

ュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取る方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了するステップと、

を有する。

【００２１】

請求項２に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【００２２】

請求項３に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【００２３】

請求項４に記載の発明では、前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【００２４】

請求項５に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００２５】

請求項６に記載の発明は、セキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【００２６】

請求項７に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００２７】

請求項８に記載の発明は、そのプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置である。

【００２８】

請求項９に記載の発明では、セキュリティポリシーに基づいた文書の読み取り装置は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、

前記読み取り装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であるかを判定する手段と

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、

を有する。

【００２９】

請求項１０に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【００３０】

請求項１１に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【００３１】

請求項１２に記載の発明では、前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【００３２】

請求項１３に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００３３】

請求項１４に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

前記組み合わせでネットワーク配信を実行する場合の要件と、
を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法であって、
前記文書を読み取り且つネットワーク配信を行う方法は、
前記ユーザ属性を取得するステップと、
読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、
取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、
前記読み取りとネットワーク配信が許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、
前記文書の読み取りとネットワーク配信が許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、
抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了するステップと、
抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行可能であるかを判定するステップと、
実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、
すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りとネットワーク配信を行って終了するステップと、
を有する。

【００３４】

請求項１５に記載の発明では、前記実行可能な要件が、前記読み取った文書データに電子透かしを埋め込むことである。

【００３５】

請求項１６に記載の発明では、前記実行対応可能な要件は、前記読み取った文

書データに表示可能なラベルを埋め込むことである。

【００３６】

請求項１７に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【００３７】

請求項１８に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００３８】

請求項１９に記載の発明では、前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【００３９】

請求項２０に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである。

【００４０】

請求項２１に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【００４１】

請求項２２に記載の発明は、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラムである。

【００４２】

請求項２３に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００４３】

請求項２４に記載の発明は、そのプログラムをコンピュータにネットワーク配

信するプログラム伝送装置である。

【００４４】

請求項２５に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせでネットワーク配信を実行する場合の要件と、

を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、

を有する。

【００４５】

請求項２６に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【００４６】

請求項２７に記載の発明では、前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【００４７】

請求項２８に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【００４８】

請求項２９に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【００４９】

請求項３０に記載の発明では、前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【００５０】

請求項３１に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持ったＰＤＦファイルである。

【００５１】

請求項３２に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【００５２】

以上本発明により、文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の印刷装置を提供することができる。

【００５３】

請求項３３に記載の発明は、ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作する入出力装置において、前記ドキュメントセキュリティポリシーを外部から設定することを特徴とする入出力装置である。

【００５４】

請求項３４に記載の発明は、前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする入出力装置である。

【００５５】

請求項３５に記載の発明は、設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とする入出力装置である。

【００５６】

請求項３６に記載の発明は、設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とする入出力装置である。

【００５７】

請求項３７に記載の発明は、外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とする入出力装置である。

【００５８】

請求項３８に記載の発明は、前記外部のサーバから前記ドキュメントセキュリ

ティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする入出力装置である。

【００５９】

請求項３９に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【００６０】

請求項４０に記載の発明は、前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に、前記入出力装置自身の認証情報を送信することを特徴とする入出力装置である。

【００６１】

請求項４１に記載の発明は、前記外部のサーバへポリシー送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とする入出力装置である。

【００６２】

請求項４２に記載の発明は、前記入出力装置の電源が投入されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【００６３】

請求項４３に記載の発明は、前記入出力装置内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【００６４】

請求項４４に記載の発明は、前記入出力装置を操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【００６５】

請求項４５に記載の発明は、取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とする入出力装置である。

【００６６】

請求項４６に記載の発明は、前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とする入出力装置である。

【００６７】

請求項４７に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする入出力装置である。

【００６８】

請求項４８に記載の発明は、前記入出力装置は、プリンタ、プリンタサーバ、スキャナ、スキャナサーバ、コピア、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とする入出力装置である。

【００６９】

請求項４９に記載の発明は、ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作するドキュメント処理ソフトウェアにおいて、前記前記ドキュメントセキュリティポリシーを外部から設定することを特徴とするドキュメント処理ソフトウェアである。

【００７０】

請求項５０に記載の発明は、ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とするドキュメント処理ソフトウェアである。

【００７１】

請求項５１に記載の発明は、設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とするキュメント処理ソフトウェアである。

【００７２】

請求項５２に記載の発明は、設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とするドキュメント処理ソフトウェアである。

【００７３】

請求項５３に記載の発明は、外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とするドキュメント処理ソフトウェアである。

【００７４】

請求項５４に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とするドキュメント処理ソフトウェアである。

【００７５】

請求項５５に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【００７６】

請求項５６に記載の発明は、前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に,前記ドキュメント処理ソフトウェア自身の認証情報を送信することを特徴とするドキュメント処理ソフトウェアである。

【００７７】

請求項５７に記載の発明は、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とするドキュメント処理ソフトウェアである。

【００７８】

請求項５８に記載の発明は、前記ドキュメント処理ソフトウェアが起動されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【００７９】

請求項５９に記載の発明は、前記ドキュメント処理ソフトウェアの内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【００８０】

請求項６０に記載の発明は、前記ドキュメント処理ソフトウェアを操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【００８１】

請求項６１に記載の発明は、取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とするドキュメント処理ソフトウェアである。

【００８２】

請求項６２に記載の発明は、前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とするドキュメント処理ソフトウェアである。

【００８３】

請求項６３に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とするドキュメント処理ソフトウェアである。

【００８４】

請求項６４に記載の発明は、前記ソフトウェアは、プラグインであることを特徴とするドキュメント処理ソフトウェアである。

【００８５】

請求項６５に記載の発明は、少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバと入出力装置からなるドキュメントシステムにおいて、前記入出力装置が前記サーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステムである。

【００８６】

請求項６６に記載の発明は、前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止或は許可する場合の要件が記述されていることを特徴とするドキュメントシステムである。

【００８７】

請求項６７に記載の発明は、前記入出力装置が前記サーバに対して、少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記入出力装置に対して、少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とするドキュメントシステムである。

【００８８】

請求項６８に記載の発明は、前記入出力装置が前記サーバに対して情報を送信する前に、前記入出力装置自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【００８９】

請求項６９に記載の発明は、前記サーバが前記入出力装置に情報を送信する前に,前記サーバ自身の認証情報を送信し、前記入出力装置は受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【００９０】

請求項７０に記載の発明は、前記入出力装置は、プリンタ、プリンタサーバ、

スキャナ、スキャナサーバ、コピア、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とするドキュメントシステムである。

【００９１】

請求項７１に記載の発明は、少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバとドキュメント処理ソフトウェアからなるドキュメントシステムにおいて、前記ドキュメント処理ソフトウェアがサーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステムである。

【００９２】

請求項７２に記載の発明は、前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とするドキュメントシステムである。

【００９３】

請求項７３に記載の発明は、前記ドキュメント処理ソフトウェアが、前記サーバに対して少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記ドキュメント処理ソフトウェアに対して少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とするドキュメントシステムである。

【００９４】

請求項７４に記載の発明は、前記ドキュメント処理ソフトウェアが前記サーバに対して情報を送信する前に、前記ドキュメント処理ソフトウェア自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【００９５】

請求項７５に記載の発明は、前記サーバが前記ドキュメント処理ソフトウェアに情報を送信する前に、前記サーバ自身の認証情報を送信し、前記ドキュメント

処理ソフトウェアは、受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【００９６】

請求項７６に記載の発明は、前記ドキュメント処理ソフトウェアは、プラグインの形態をとることを特徴とするドキュメントシステムである。

【００９７】

以上のように、本発明により、読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機等に、セキュリティーポリシーを外部より設定することも可能である。

【００９８】

【発明の実施の形態】

本発明の実施例を、以下に詳細に説明する。

【００９９】

先ず最初に、本発明の第１の実施例のセキュリティポリーシーについて説明する。

【０１００】

本実施例では、異なるタイプのシステムでドキュメントに対するセキュリティポリシーを共有するために、以下のような仕組みを使用して、セキュリティポリシーを記述する。ここでは、記述したセキュリティポリシーのことをドキュメントセキュリティポリシー（DSP）と呼ぶ。

【０１０１】

図１は、セキュリティポリシーの例を示す。ユーザの属する組織は、例えば、機密文書、丸秘文書、社外秘文書のような、文書の機密レベルごとに、ドキュメントに対して、例えば、図１のようなセキュリティポリシーを掲げることが想定される。

【０１０２】

このようなポリシーをDSPとして記述できるようにするために，以下のような方法を使用する。

【０１０３】

まず最初に、ドキュメントを機密レベル（極秘、丸秘、社外秘など）と、カテゴリ（人事文書、技術文書など）に応じて分類する。この、機密レベルとカテゴリの組みを、ドキュメントのセキュリティラベルと呼ぶ。このセキュリティラベルは、実際には、個々のドキュメントに属性情報として付与される。

【０１０４】

上記のような、分類の仕方の一例を、図１６に示す。図１６は、document_label_terminology.xmlファイルのリストの例を示す。

【０１０５】

DSPには、ドキュメントの機密レベル及びカテゴリに応じて、ドキュメントに対して許可される操作（オペレーション）を規定し、そして、その操作を許可する際に実行されるべき要件（管理責任者の許可を得る、ラベルを印刷する、など）を指定できるようにする必要がある。そのような、ドキュメントの機密レベル及びカテゴリを記述するのが、図２のdocument_label_terminology.xmlファイルである。図２においては、社内一般文書、人事関連文書及び技術関連文書のような、文書カテゴリの種類が設けられている。また、社外秘、秘、極秘のような、文書のセキュリティレベルの種類が設けられている。

【０１０６】

図３から図１３は、policy_terminology.xmlファイルのリストの例を示す図（１）から（１１）を示す。図３から図１３により、１つのpolicy_terminology.xmlファイルを構成する。

【０１０７】

図３から図１３のpolicy_terminology.xmlファイルのリストの例に示すように、policy_terminology.xmlファイルは、システムタイプの分類を記述する。そして、そのシステムタイプごとに、オペレーションを列挙する。そして、そのオペレーションごとに、オペレーションの実行の際にサポート可能な要件を列挙しておく。例えば、図３においては、システムタイプの種類として、複写機、プリンタ、ファクシミリ、スキャナ等が記述される。そして、例えば、図４に示されたように、複写機に関わるオペレーションとして、紙から紙への複写等が記述される。更に、例えば、図６に示すように、複写に関わる要件として、明示な許可、

監査証跡の記録等が記述される。

【０１０８】

図１４から図２３は、policy.xmlのファイルのリストの例を示す図（１）から（１０）を示す。図１４から図２３により、１つのpolicy.xmlのファイルを構成する。

【０１０９】

上述の図２に示す定義ファイルdocument_label_terminology.xmlと、図３から図１３のpolicy_terminology.xmlファイルをもとにして、ユーザ組織のセキュリティに対するポリシーをDSPとして例えば図１４から図２３に示すpolicy.xmlファイルのリストのように記述する。

【０１１０】

次に、図１４から図２３のpolicy.xmlファイルのリストに示された、DSPの構造を、図２４から２６を参照して、以下に、詳しく説明する。

【０１１１】

図２４は、DSPの識別情報の例を示す図である。図１４に示されたpolicy.xmlのファイルのリストの例に記載されているように、DSPの先頭には、そのDSPの識別情報を記述する。DSPの識別情報は、図２４に示されたように、<about_this_policy>と、</about_this_policy>で囲まれた範囲に記載される。

【０１１２】

DSPの識別情報には、先ず最初に、このDSPを他のDSPと区別するために必要な、シリアル番号を、

<serial_number>RDSP0100-00000000000012-2023</serial_number>に示すように、記述する。

【０１１３】

次に、適用した定義ファイルであるpolicy_terminology.xmlファイルのシリアル番号を、

<terminology_applied>RDST0100-00000000000001-9487</terminology_applied>のように記述する。定義ファイルについても更新される可能性があるため、このDSPがどの定義ファイルに基づいて記述されているのかを明確にするために記録

しておく。

【０１１４】

次に、このDSPのタイトル、バージョン番号、作成日時、作成者、説明といった一般的な書誌情報を記録する。

【０１１５】

そして、DSPの識別情報は、</about_this_policy>により終了する。

【０１１６】

次に、上述のDSPの識別情報に続いて、ポリシーの内容を<policy>と</policy>で囲まれた範囲に記述する。図２５は、ポリシーの内容を示す一実施例を示す。

【０１１７】

ポリシーの内容は、以下に説明するように、階層構造を用いて記録する。

【０１１８】

ポリシー<policy>は、複数のアクセス制御ルール<acc_rule>で構成される．一つのアクセス制御ルール<acc_rule>は、対象とするドキュメントのカテゴリ<doc_category>とレベル<doc_security_level>を一意に指定し，さらにアクセス制御リスト<acl>を一つ含むように構成される。

【０１１９】

アクセス制御リスト<acl>は、複数のアクセス制御エレメント<ace>で構成される。

【０１２０】

各アクセス制御エレメント<ace>は、対象とするユーザのカテゴリ<user_category>とレベル<user_security_level>を一意に指定し，さらに複数のオペレーション<operation>で構成される。

【０１２１】

各<operation>は、一つのオペレーション名<name>と、一つの禁止<denied/>、または一つの許可<allowed/>、または複数の<requirement>で構成される。

【０１２２】

ドキュメントのカテゴリ<doc_category>やユーザのカテゴリ<user_category_level>に記述している”ANY”は、どのカテゴリ、及び、レベルにも適用されるこ

とを示している。また、ユーザのカテゴリ<user_category>の”DOC-CATEGORY”は、ユーザのカテゴリがドキュメントのカテゴリと同じときに適用されることを示している。

【０１２３】

この実施例では、禁止するオペレーションには<denied/>を指定するようにしているが、DSPに記載されていなければアクセスは許可されていないことを表している、というように構成してもよい。

【０１２４】

このように、DSPを記述することにより、ドキュメントのタイプ（カテゴリ、レベル）に応じて，どのようなユーザタイプ（カテゴリ、レベル）が、ドキュメントに対してどのようなオペレーションが可能なのかを記述できる。そして更に、そのドキュメントについて、ユーザが、オペレーションが可能な場合には、どのような要件を満たさなければならないのかを明確に記述することができる。

【０１２５】

そして、DSPを、上記のようにプラットフォームに依存しないXMLで記述することにより、異なるタイプのシステム間で、このDSPを共通に利用することができる。特に、セキュリティポリシーを適用したい対象は、電子的なドキュメントに限らず、紙のドキュメントに対しても適用できなければならないため、図３から図１３のpolicy_terminology.xmlファイルや図１５から図２３のpolicy.xmlファイルに記述しているように、紙ドキュメントに関するオペレーション（hardcopy，scanなど）も規定できる。

【０１２６】

本実施例の、図２５に示す要件の中に、以下の<requirement>explicit_authorization</requirement>

が存在する。これは、「ドキュメントの管理責任者により明示的な許可が得られた場合には、そのオペレーションを許可する」という要件である。すべて、このDSPに従ってオペレーションがコントロールされるようになると、自由度が無くなる恐れが生じる。しかし、この明示的な許可という要件を指定できるようにすることにより、柔軟なオペレーションコントロールが可能となる。

【０１２７】

また、本実施例の特徴として、その「明示的な許可」という要件を指定可能にすることによって、明示的な許可が得られれば実行してもよいオペレーションと，明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができるということである。

【０１２８】

従って、DSPに記載しないか又は、<denied/>で指定されたオペレーションは明示的な許可が得られたとしても禁止しなければならないオペレーションである。これにより、ポリシーを記述している側の意図を、的確に規定できるようになり、誤って許可を与えてしまってオペレーションが実行されてしまうというような事態をあらかじめ防ぐように規定することができる。

【０１２９】

次に本発明のDSPの別の記述形式の実施例を、図２６に示す。無条件で許可するオペレーションや、禁止するオペレーションが多くなった場合には、オペレーションごとに<operation><allowed/></operation>というような入れ子構造を記述するのは効率が悪いので、無条件で許可するオペレーションを列挙する、<allowed_operations>と、許可しないオペレーションを列挙する、<denied_operations>を使用するようにしても良い。

【０１３０】

図２７は、上述のDSPを蓄積し且つ配布する種々の媒体を示す。

【０１３１】

以上で説明したように、図２７に示されたDSP５０は、XML（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）で記述されている。そして、電子的なファイルとして記録しておくことができる。また、その電子的なファイルを格納した、例えば、ハードディスク５１、光磁気ディスク５２、フレキシブルディスク５３、又は、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ、ＤＶＤ＋Ｒのような光ディスク５４のような記憶媒体を作成することができる。また、その電子的なDSPをコンピュータ５５を使用して、ネットワーク５６を介してで伝送することができる。

【０１３２】

このDSPは、特定のシステム向けのセキュリティポリシーの記述ではなく、異なる複数のシステムで共通に利用できるセキュリティポリシーの記述である。従って、このセキュリティポリシー記述を記憶した記憶媒体を作成し、そして配布したり又は、ネットワーク経由して伝送したりすることにより、複数のシステムで共通に利用しやすくなる。

【０１３３】

次に、本発明の第２の実施例について説明する。図２８は、本発明のセキュリティーポリシーに基づいて動作する入出力装置の一例としての読取装置の実施例について説明する。しかし本発明は、他の入出力装置である、印刷装置や複写装置にも適用できる。

【０１３４】

本発明の第２の実施例を、図２８及び図２９を参照して以下に詳細に説明する。

【０１３５】

図２８は、本発明の実施例の文書読み取り装置の構成を示す図である。また、図２９は、ＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）により記述した、本発明の実施例のセキュリティポリシーを示す。

【０１３６】

図２８に示す本発明の実施例の文書読み取り装置１００は、主に、オペレーションパネル１０１、データベース１０２、ユーザ属性取得手段１０３、文書属性取得手段１０４、セキュリティーポリシー１０５、読み取り手段１０６、読み取りデータ１０７及びネットワークポート１０８より構成される。

【０１３７】

オペレーションパネル１０１には、読み取り支持１１０が入力される。

【０１３８】

図２８においては、読み取り装置は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。また、以下に説明する本発明の実施例をコン

ピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記録媒体に記録され、その実行前に、コンピュータにより読みこまれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【０１３９】

図２９は、ＸＭＬにより記述した、セキュリティポリシーであり、つぎのようにルール１からルール３を示す。

【０１４０】

ルール１は、図２９の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１１行目<operation>から、第１４行目</operation>までの部分により記述される。

【０１４１】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール１が適用されることを示す。

【０１４２】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【０１４３】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないこととを示す。

【０１４４】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１４５】

更に第１２行目と第１３行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【０１４６】

従って、ルール１では、第５行目、第６行目、第９行目、第１０行目、第１２行目及び第１３行目により、文書カテゴリーにかかわりなく、文書のセキュリテ

ィレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは要件なく許可される。

【０１４７】

次に、ルール２は、図２９の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１５行目<operation>から、第２０行目</operation>までの部分により記述される。

【０１４８】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール２が適用されることを示している。

【０１４９】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【０１５０】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないことを示す。

【０１５１】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１５２】

更に、第１６行目から第１９行目の

<name>net_delivery</name>

<requirement>audit</requirement>

<requirement>print_restriction</requirement>

<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【０１５３】

従って、ルール２では、第５行目、第６行目、第９行目、第１０行目、第１６

行目から第１９行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、ネットワーク配信は、ログを記録することと、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【０１５４】

そして、ルール３は、図２９の第２４行目の<acc_rule>から、第３０行目の<user_security_level>ANY</user_security_level>までの部分及び、第３１行目<operation>から、第３５行目</operation>までの部分により記述される。

【０１５５】

第２５行目の<doc_category>ANY</doc_category>は、文書カテゴリーにかかわりないことを示す。

【０１５６】

第２６行目の<doc_security_level>high</doc_security_level>は、
文書のセキュリティレベルがhighの場合を示す。

【０１５７】

第２９行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリーが文書のカテゴリーと同じであることを示す。

【０１５８】

第３０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１５９】

第３２行目から第３４行目の、

<name>scan</name>

<requirement>audit</requirement>

<requirement>embed_trace_info</requirement>

は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。

【０１６０】

従って、ルール３では、第２５行目、第２６行目、第２９行目、第３０行目、第３１行目から第３４行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”high”の場合には、ユーザのカテゴリーが文書のカテゴリーと同じであり、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。

【０１６１】

ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。

【０１６２】

次に、図２９に示したセキュリティポリシーを使用して、図２８に示した本発明の実施例の文書読み取り装置が文書を読み取り又は、読み取った文書をネットワークに配信する場合の実施例について説明する、

先ず最初に、文書読み取り装置が文書を読み取る場合の実施例について説明する。

【０１６３】

先ず最初に、ステップＡ１で、ユーザが、読み取り装置１００に紙文書を設置し、オペレーションパネル１０１から、紙文書の読み取り指示１１０を入力する。

【０１６４】

次に、ステップＡ２で、読み取り手段１０６が、紙文書の読み取りを行う。

【０１６５】

次に、ステップＡ３で、文書属性取得手段１０４は、読み取った文書データのバーコードや電子透かしなどの画像情報から、文書ＩＤを抽出し、データベース１０２に登録されている文書ＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【０１６６】

次に、ステップＡ４で、読み取り手段１０６は、上記の文書属性取得手段１０４が通知した文書属性に従って、セキュリティポリシー１０５の中の対応するエントリを検索して、要件を抽出する。

【０１６７】

上述の図２９に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”basic”の文書を読み取りしようとしている場合には、抽出すべき要件はない。

【０１６８】

また、上述の図２９に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。

【０１６９】

次に、ステップＡ５－１で、上述のステップ４のセキュリティレベルが”basic”のときの場合のように、抽出すべき要件がない場合には、読み取り手段は文書の読み取りを行って、ユーザは文書データを取得して終了する。

【０１７０】

一方、ステップＡ５－２では、上述のステップ４のキュリティレベルが”high”のときの場合のように、抽出すべき要件がある場合には、読み取り手段はその要件をすべて満たすことができるかを判定する。

【０１７１】

ステップＡ５－２の場合には、次に以下のステップ６－１と６－２が実行される。

【０１７２】

ステップＡ６－１では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【０１７３】

次に、ステップＡ６－２では、すべての要件を満たすことができる場合は、その要件を満たした読み取りを行って、ユーザは文書データを取得して終了する。この場合には、ステップＡ６－２では、以下のステップ、Ａ７－１からＡ７－６が実行される。

【０１７４】

ステップＡ７－１では、ユーザ属性取得手段１０３は、オペレーションパネル１０１から読み取り指示１１０を出したユーザに、ユーザＩＤの入力要求を出す。

【０１７５】

次に、ステップＡ７－２では、ユーザは、オペレーションパネル１０１からユーザＩＤを入力する。

【０１７６】

次に、ステップＡ７－３では、ユーザ属性取得手段１０３は、ユーザＩＤからデータベース１０２に登録されている入力されたユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【０１７７】

次に、ステップＡ７－４では、ログを記録する。

【０１７８】

そして、ステップＡ７－５では、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【０１７９】

最後に、ステップＡ７－６で、ユーザは文書データを、読み取りデータ１０７内に取得して終了する。

【０１８０】

以上のように、図２９に示したセキュリティポリシーを使用して、図２８に示した本発明の実施例の文書読み取り装置が文書を読み取ることができる。

【０１８１】

次に、文書読み取り装置が文書を読み取り且つ読み取った文書をネットワークに配信する場合の実施例について説明する。

【０１８２】

先ず最初に、ステップＢ１で、ユーザが、読み取り装置１０６に紙文書をセットし、オペレーションパネル１０６から、読み取りデータの配信先の指定及び紙文書の読み取り指示１１０を出す。

【０１８３】

次に、ステップＢ２で、読み取り手段１０６が、紙文書の読み取りを行う。

【０１８４】

次に、ステップＢ３で、文書属性取得手段１０４は、読み取った文書データのバーコードや電子透かしなどの画像情報から文書ＩＤを抽出し、データベース１０２に登録されている文書ＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【０１８５】

次に、ステップＢ４では、読み取り手段１０６は、上記の文書属性取得手段１０４が通知した文書属性に従って、セキュリティポリシー１０５の中の対応するエントリを検索し、要件を抽出する。

【０１８６】

上述の図２９に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”basic”の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【０１８７】

また、上述の図２９に示すセキュリティポリシーに基づいて、例えば、セキュ

リティレベルが”high”の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと(例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【０１８８】

次に、例えば、文書をネットワークへ配信する際の要件が、セキュリティーポリシー１０５内に存在しない場合には、ステップＢ５－１では、読み取り手段１０６は文書をネットワークポート１０８を介してネットワークへ配信して、処理を終了する。

【０１８９】

一方、例えば、文書をネットワークへ配信する際の要件が、セキュリティーポリシー１０５内に存在する場合には、ステップ５－２で、読み取り手段１０６が、その要件をすべて満たすことができるかを判定する。

【０１９０】

ステップＢ５－２の場合には次に、ステップＢ５－３で、ネットワークに配信することを許可するルールがない場合には、読み取り手段１０６が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、読み取りデータを破棄して終了する。例えば、これは、上述のステップＢ４の、セキュリティレベルが”high”の場合である。

【０１９１】

次に、ステップＢ６－１では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【０１９２】

次に、ステップＢ６－２では、例えば、上述のセキュリティレベルが”basic”の場合のように、すべての要件を満たすことができる場合は、その要件を満たした読み取り及び、文書をネットワークに配信して終了する。この場合には、ステップＢ６－２では、以下のステップ、Ｂ７－１からＢ７－６が実行される。

【０１９３】

ステップＢ７－１では、ユーザ属性取得手段１０６は、オペレーションパネル１０１から、読み取り指示１１０を出したユーザに、ユーザＩＤの入力要求を出す。

【０１９４】

次に、ステップＢ７－２では、ユーザは、オペレーションパネル１０１からユーザＩＤを入力する。

【０１９５】

次に、ステップＢ７－３では、ユーザ属性取得手段１０３は、ユーザＩＤからデータベース１０２に登録されている入力されたユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段１０６に通知する。

【０１９６】

次に、ステップＢ７－４では、ログを記録する。

【０１９７】

そして、ステップＢ７－５では、読み取った文書データを、印刷不可能なデータ(たとえばADOBE（登録商標）の印刷禁止属性を持ったPDFなど)に変換する。

【０１９８】

最後にステップＢ７－６では、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、文書を、ネットワークポート１０８を介してネットワークへ配信し、終了する。

【０１９９】

以上のように、図２９に示したセキュリティポリシーを使用して、図２８に示した本発明の実施例の文書読み取り装置が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【０２００】

次に、本発明のセキュリティポリシーを、入出力装置の一例としての、上述の読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機に設定する実施例について、以下に説明する。

【０２０１】

次に、本発明の第３の実施例について説明する。図３０は、本発明の第３の実

施例を示す図である。図３０は、ネットワークポートを通じて外部からセキュリティポリシーを受信し、内部のポリシーＤＢ（データターベース）に保存する複合機３０００の実施例である。図３０に示す複合機３０００は、上述した、読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機を構成する。複合機３０００は、複合機エンジン３００１、ＣＰＵ（中央処理装置）３００２、ポリシーＤＢ３００３、アプリケーション３００４及びネットワーク３００６に接続されたネットワークポート３００５より構成される。

【０２０２】

ＣＰＵ３００２は、アプリケーション３００４の指示に従って、ネットワークポート３００５を通じて外部からポリシーを受信し、内部のポリシーＤＢ３００３に保存する。ネットワークプロトコルは、例えば、TCP/IP、HTTP+XML(SOAP)などのどのような標準的なプロトコルを利用することもできる。もちろん、FTPやMAILなどのプロトコルを利用しても良い。

【０２０３】

複合機の動作は、アプリケーション３００４により制御される。ＣＰＵ３００２は、アプリケーション３００４からの指示に従って動作する。ＣＰＵ３００２は、ポリシーＤＢ３００３から蓄積されているポリシーを読み出す。そして、読み出したポリシーに記載されているルールに従って、複合機エンジン３００１を制御し、そして、アプリケーション３００４の指示を実現する。すなわち、ポリシーに記載されているルールに従って複合機３０００の動作を制御する。

【０２０４】

次に、本発明の第４の実施例について説明する。図３１は、本発明の第４の実施例を示す図である。図３１は、取り外し可能な記憶媒体を通じて外部からポリシーを取得し、内部のポリシーＤＢ（データターベース）に保存する複合機３０００の実施例である。図３１に示す複合機３０００は、上述した、読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機を構成する。複合機３０００は、複合機エンジン３００１、ＣＰＵ（中央処理装置）３００２、ポリシーＤＢ３００３、アプリケーション３００４及び取り外し可能な記憶媒体３１０１により構成される。図３１において、ＣＰＵ３００２は、アプリケーション３００

４に指示に従って、取り外し可能な記憶媒体３１０１に記憶されているセキュリティーポリシーを読み出して、内部のポリシーＤＢ３００３に保存する。内部のポリシーＤＢ３００３にセキュリティーポリシーが記憶された後の動作は、上述の第３の実施例と同様である。

【０２０５】

取り外し可能な記憶媒体３１０１の例は、メモリカード、フレキシブルディスク、光ディスクなどのような標準的な記憶媒体を使用することができる。

【０２０６】

次に、本発明の第５の実施例について説明する。図３２は、本発明の第５の実施例を示す。図３２は、複合機３０００に、ネットワーク３００６を介して、セキュリティポリシーを設定するシステム３２００の実施例を示す。図３２に示すシステムは、複合機３０００、ネットワーク３００６、管理コンソール３２０１及びポリシー管理サービス３２０２から構成される。

【０２０７】

先ず最初に、セキュリティポリシーを設定するシステム３２００の管理者は、管理コンソール３２０１からポリシー管理サービス３２０２へポリシーを設定する。

【０２０８】

次に、ポリシー管理サービス３２０２は、複合機３０００へネットワーク３００６を介して設定されたポリシーを送信する。

【０２０９】

そして、複合機３０００は、ネットワーク３００６を介してポリシー管理サービス３２０２から受信したポリシーに従って動作する。

【０２１０】

このような構成の場合に、複合機３０００は、ポリシーを送信するポリシー管理サービス３２０２が信頼できるものであるかどうかを確かめることで、間違ったポリシーの受信や悪意あるポリシーの設定などを防ぐこともできる。すなわち、ポリシー管理サービス３２０２がポリシーの配布をする時に、以下のような動作を実行する。

【０２１１】

先ず最初に、ポリシー管理サービス３２０２は、自分自身の認証情報とポリシーを複合機３０００に送信する。

【０２１２】

次に、複合機３０００は送信されたポリシー管理サービス３２０２の認証情報を検証する。

【０２１３】

そして、このポリシー管理サービス３２０２の認証情報が正しいと確認された場合には、送信されたポリシーを正式なものとして利用する。

【０２１４】

このような動作を実行することにより、複合機３０００は、間違ったポリシーの受信や悪意あるポリシーの設定などを防ぐこともできる。

【０２１５】

次に、本発明の第６の実施例について説明する。図３３は、本発明の第６の実施例を示す。本実施例は、複合機を、最初にネットワークに接続した場合などのように、まだセキュリティポリシーを持っていない場合の複合機の動作の実施例を示す。

【０２１６】

図３３に示すシステム３２００は、複合機３０００に、ネットワーク３００６を介して、セキュリティポリシーを設定するシステム３２００の実施例を示す。図３３に示すシステムは、複合機３０００、ネットワーク３００６、管理コンソール３２０１及びポリシー管理サービス３２０２から構成される。本実施例は、以下のように実行される。

【０２１７】

先ず最初に、複合機３０００の電源が投入される。

【０２１８】

次に、複合機３０００はポリシー管理サービス３２０２からポリシーを取得する。

【０２１９】

そして、複合機３０００は、ポリシー管理サービス３２０２取得したポリシーに従って動作する。

【０２２０】

このような場合には、ポリシーを受信する複合機３０００が信頼できるものであるかどうかを確かめることで余分な情報の漏洩(ここではポリシー)を防ぐこともできる。すなわち、複合機３０００が最初に、ポリシー管理サービス３２０２からポリシーを取得をする時に、以下のような動作を実行する。

【０２２１】

先ず最初に、複合機３０００は、自分自身の認証情報とポリシーの取得要求をポリシー管理サービス３２０２に送信する。

【０２２２】

次に、ポリシー管理サービス３２０２は、送信された複合機３０００の認証情報を検証する。

【０２２３】

そして、この複合機３０００の認証情報が正しいと、ポリシー管理サービス３２０２が確認した場合には、複合機３０００にポリシーを送信する。

このような動作を実行することにより、ポリシー管理サービス３２０２は、余分な情報の漏洩(ここではポリシー)を防ぐこともできる。

【０２２４】

次に、本発明の第７の実施例について説明する。図３４は、本発明の第７の実施例を示す。本実施例は、上述の第５の実施例と第６の実施例に示すように、ポリシーを配布する及び、ポリシーを取得するというような、２通りの動作を実現するためには、ポリシー管理サービス３２０２側と、複合機３０００側に、２通りのネットワークアプリケーションを用意する必要がある。本実施例では、このような２つの動作を、一つのアプリケーションで行うことができる。

【０２２５】

図３４に示すシステム３２００は、複合機３０００、ネットワーク３００６、管理コンソール３２０１及びポリシー管理サービス３２０２から構成される。

【０２２６】

本実施例の動作を以下に説明する。

【０２２７】

先ず最初に、システム３２００の管理者は、管理コンソール３２０１からポリシー管理サービス３２０２へポリシーを設定する。

【０２２８】

次に、ポリシー管理サービス３２０２は、ポリシー配布通知を複合機３０００へ送信する。

【０２２９】

そして、複合機３０００は、ポリシー管理サービス３２０２からポリシーを取得する。

【０２３０】

最後に、複合機３０００は、取得したポリシーに従って動作する。

【０２３１】

以上のように、このような２つの動作を、一つのアプリケーションで行うことができる。

【０２３２】

次に、本発明の第８の実施例について説明する。図３５は、本発明の第８の実施例を示す。本実施例は、頻繁に電源を切断又は再投入する場合には、前述の実施例のように、その度に、複合機３０００がポリシー管理サービス３２０２からポリシーを取得していたのでは、効率が悪い場合がある。そのような場合には、以下のように実行することができる。

【０２３３】

図３５に示すシステム３２００は、複合機３０００、ネットワーク３００６、管理コンソール３２０１、ポリシー管理サービス３２０２及び、複合機３０００に内蔵又は、接続されたタイマー装置３５０１から構成される。

【０２３４】

第１のステップでは、最初に、複合機３０００の内部に、ポリシーを取得する時間間隔(あるいは取得時刻)を予め設定する。

【０２３５】

そして、第１のステップでは、更に、複合機３０００の通電中に、タイマー装置３５０１が、設定時刻の経過を検知する。

【０２３６】

第２のステップでは、第１のステップで検知された設定時刻に、複合機３０００は、ポリシー管理サービス３２０２からポリシーを取得する。

【０２３７】

そして、第３のステップで、複合機３０００は、取得したポリシーに従って動作する。

【０２３８】

このように、動作することにより、設定時刻において、複合機３０００は、ポリシー管理サービス３２０２からポリシーを取得するので、電源の再投入の度に、ポリシーを取得することはなく、これにより、効率を向上することができる。

【０２３９】

次に、本発明の第９の実施例について説明する。図３６は、本発明の第９の実施例を示す。本実施例は、ポリシーのサイズや回線の速度に依存して、ポリシーをオフラインで設定する場合の実施例を示す。

【０２４０】

本実施例では、先ず最初に、オフラインで、複合機３０００に、ポリシーを設定する。

【０２４１】

次に、複合機３０００は設定されたポリシーに従って動作する。

【０２４２】

オフラインでポリシーを設定する場合には、それに応じたオフラインメディアのI/F（インターフェース）を複合機に設ける。また、オフラインでポリシーを設定する場合には、そのポリシーに、改ざん検知コードなどを追加することにより、ポリシーの信頼性を向上することもできる。

【０２４３】

次に、本発明の第１０の実施例について説明する。図３７は、本発明の第１０の実施例を示す。本実施例は、オフラインで設定したポリシーを切り替えて利用

する場合の実施例を示す。

【０２４４】

図３７に示すシステム３２００は、複合機３０００、ネットワーク３００６、管理コンソール３２０１及びポリシー管理サービス３２０２から構成される。

【０２４５】

先ず最初に、オフラインで、複合機３０００に、１つ以上のポリシーを予め設定する。

【０２４６】

次に、管理コンソール３２０１から、ポリシー管理サービス３２０２に、ポリシーを設定する。

【０２４７】

そして、次に、ポリシー管理サービス３２０２は、複合機３０００に、設定されたポリシーの選択情報を通知する。

【０２４８】

最後に、複合機３０００は、ポリシー管理サービス３２０２０により通知された、選択されたポリシーに従って動作する。

【０２４９】

本実施例により、オフラインで設定したポリシーを切り替えて利用することができる。

【０２５０】

【発明の効果】

以上説明したように、本発明によって、セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置及びネットワーク配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、伝送装置及び、セキュリティポリシーを外部から設定する入出力装置を提供することができる。

【図面の簡単な説明】

【図１】

セキュリティポリシーの例を示す図である。

【図２】

document_label_terminology.xmlのファイルのリストの例を示す図である。

【図３】

policy_terminology.xmlのファイルのリストの例を示す図（１）である。

【図４】

policy_terminology.xmlのファイルのリストの例を示す図（２）である。

【図５】

policy_terminology.xmlのファイルのリストの例を示す図（３）である。

【図６】

policy_terminology.xmlのファイルのリストの例を示す図（４）である。

【図７】

policy_terminology.xmlのファイルのリストの例を示す図（５）である。

【図８】

policy_terminology.xmlのファイルのリストの例を示す図（６）である。

【図９】

policy_terminology.xmlのファイルのリストの例を示す図（７）である。

【図１０】

policy_terminology.xmlのファイルのリストの例を示す図（８）である。

【図１１】

policy_terminology.xmlのファイルのリストの例を示す図（９）である。

【図１２】

policy_terminology.xmlのファイルのリストの例を示す図（１０）である。

【図１３】

policy_terminology.xmlのファイルのリストの例を示す図（１１）である。

【図１４】

policy.xmlのファイルのリストの例を示す図（１）である。

【図１５】

policy.xmlのファイルのリストの例を示す図（２）である。

【図１６】

policy.xmlのファイルのリストの例を示す図（３）である。

【図１７】

policy.xmlのファイルのリストの例を示す図（４）である。

【図１８】

policy.xmlのファイルのリストの例を示す図（５）である。

【図１９】

policy.xmlのファイルのリストの例を示す図（６）である。

【図２０】

policy.xmlのファイルのリストの例を示す図（７）である。

【図２１】

policy.xmlのファイルのリストの例を示す図（８）である。

【図２２】

policy.xmlのファイルのリストの例を示す図（９）である。

【図２３】

policy.xmlのファイルのリストの例を示す図（１０）である。

【図２４】

DSPの識別情報の例を示す図である。

【図２５】

ポリシーの内容を示す一実施例を示す図である。

【図２６】

本発明のDSPの別の記述形式の実施例を示す図である。

【図２７】

DSPを蓄積し且つ配布する種々の媒体を示す図である。

【図２８】

本発明の実施例の文書読み取り装置の構成を示す図である。

【図２９】

ＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）により記述した、本発明の実施例のセキュリティポリシーを示す図である。

【図３０】

本発明の第３の実施例を示す図である。

【図３１】

本発明の第４の実施例を示す図である。

【図３２】

本発明の第５の実施例を示す図である。

【図３３】

本発明の第６の実施例を示す図である。

【図３４】

本発明の第７の実施例を示す図である。

【図３５】

本発明の第８の実施例を示す図である。

【図３６】

本発明の第９の実施例を示す図である。

【図３７】

本発明の第１０の実施例を示す図である。

【符号の説明】

５０　DSP

５１　ハードディスク

５２　光磁気ディスク

５３　フレキシブルディスク

５４　光ディスク

５５　コンピュータ

５６　ネットワーク

１００　文書読み取り装置

１０１　オペレーションパネル

１０２　データベース

１０３　ユーザ属性取得手段

１０４　文書属性取得手段

１０５　セキュリティーポリシー

１０６　読み取り手段
１０７　読み取りデータ
１０８　ネットワークポート
１１０　読み取り指示
３０００　複合機
３００１　複合機エンジン
３００２　ＣＰＵ
３００３　ポリシーＤＢ
３００４　アプリケーション
３００５　ネットワークポート
３００６　ネットワーク
３２０１　管理コンソール
３２０２　ポリシー管理サービス
３５０１　タイマー装置

【書類名】　図面

【図１】

セキュリティポリシーの例を示す図

極秘文書について：
原則複写禁止（複写する際には管理責任者の許可を得なければならない），また，複写したことを記録しておかなければならない
プリントする際には複写禁止であることを示す透かしを入れなければならない，また，プリントしたことを記録しておかなければならない
閲覧は関係者のみ許可

丸秘文書について：
複写は関係者のみ許可
プリントする際には丸秘文書であることを示すラベルを同時に印刷しなければならない
閲覧は関係者のみ許可

社外秘文書について：
社外へ送付する際には管理責任者の許可を得なければならない
複写・プリント・閲覧は社内であれば許可不要

人事関連文書について：
すべて丸秘文書として取り扱う

【図２】

document_label_terminology.xmlのファイルのリストの例を示す図

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_label_terminology>
<about_this_terminology>
        <serial_number>RDST0100-00000000000001-
0001</serial_number>
        <title>Office System Research and Development Center,
DOCUMENT-LABEL-TERMINOLOGY</title>
        <version>1.00</version>
        <creation_date>2001/12/21 13:37:18</creation_date>
        <creator>Yoichi Kanai</creator>
        <description>This    is    a    sample    document-label
terminology.</description>
</about_this_terminology>
<enumeration>
        <enum_id>doc_category</enum_id>
        <enum_name>Document Category</enum_name>
        <description>文書カテゴリの種類</description>
        <item>
                <name>internal_doc</name>
                <description>社内一般文書</description>
        </item>
        <item>
                <name>human_resource_doc</name>
                <description>人事関連文書</description>
        </item>
        <item>
                <name>technical_doc</name>
                <description>技術関連文書</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>doc_security_level</enum_id>
        <enum_name>Document Security Level</enum_name>
        <description>文書のセキュリティレベルの種類</description>
        <item>
                <name>basic</name>
                <description>社外秘</description>
        </item>
        <item>
                <name>meium</name>
                <description>秘</description>
        </item>
        <item>
                <name>high</name>
                <description>極秘</description>
        </item>
</enumeration>
</document_label_terminology>
```

【図３】

policy_terminology.xmlのファイルのリストの例を示す図（1）

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<policy_terminology>
<about_this_terminology>
      <serial_number>RDST0100-00000000000001-
9487</serial_number>
      <title>Office System Research and Development Center,
DOCUMENT-SECURITY-POLICY-TERMINOLOGY</title>
      <version>1.00</version>
      <creation_date>2001/12/21 13:37:18</creation_date>
      <creator>Yoichi Kanai</creator>
      <description>This is a sample policy
terminology.</description>
</about_this_terminology>

<!-- システムタイプの列挙 -->
<enumeration>
      <enum_id>system_type</enum_id>
      <enum_name>System Type</enum_name>
      <description>システムタイプの種類</description>
      <item>
            <name>Copier</name>
            <description>複写機</description>
            <operation>copier_operation</operation>
      </item>
      <item>
            <name>Printer</name>
            <description>プリンタ</description>
            <operation>printer_operation</operation>
      </item>
      <item>
            <name>Facsimile</name>
            <description>ファクシミリ</description>
            <operation>fax_operation</operation>
      </item>
      <item>
            <name>Scanner</name>
            <description>スキャナ</description>
            <operation>scanner_operation</operation>
      </item>
      <item>
            <name>Document Repository</name>
            <description>文書リポジトリ</description>
            <operation>repository_operation</operation>
      </item>
      <item>
            <name>E-Meeting</name>
            <description>電子会議システム</description>
            <operation>emeeting_operation</operation>
```

【図４】

policy_terminology.xmlのファイルのリストの例を示す図(2)

```
        </item>
</enumeration>

<!-- システムタイプごとのオペレーションの列挙 -->
<enumeration>
        <enum_id>copier_operation</enum_id>
        <enum_name>Copier Operation</enum_name>
        <description>複写機に関わるオペレーション</description>
        <item>
                <name>hardcopy</name>
                <description>紙から紙への複写</description>
                <requirement>hardcopy_requirement</requirement>
        </item>
</enumeration>
<enumeration>
        <enum_id>printer_operation</enum_id>
        <enum_name>Printer Operation</enum_name>
        <description>プリンタに関わるオペレーション</description>
        <item>
                <name>print</name>
                <description>電子文書を紙へ印刷</description>
                <requirement>print_requirement</requirement>
        </item>
</enumeration>
<enumeration>
        <enum_id>fax_operation</enum_id>
        <enum_name>Facsimile Operation</enum_name>
        <description>ファクスに関わるオペレーション</description>
        <item>
                <name>fax_send</name>
                <description>ファクスの送信</description>
                <requirement>fax_send_requirement</requirement>
        </item>
        <item>
                <name>fax_receive</name>
                <description>ファクスの受信</description>

        <requirement>fax_receive_requirement</requirement>
        </item>
</enumeration>
<enumeration>
        <enum_id>scanner_operation</enum_id>
        <enum_name>Scanner Operation</enum_name>
        <description>スキャナに関わるオペレーション</description>
        <item>
                <name>scan</name>
                <description>紙文書をスキャンして電子文書にする
</description>
                <requirement>scan_requirement</requirement>
        </item>
</enumeration>
```

【図５】

policy_terminology.xmlのファイルのリストの例を示す図(3)

```
<enumeration>
        <enum_id>repository_operation</enum_id>
        <enum_name>Document Repository Operation</enum_name>
        <description>文書リポジトリに関わるオペレーション
</description>
        <item>
                <name>store</name>
                <description>保存する</description>
                <requirement>store_requirement</requirement>
        </item>
        <item>
                <name>revise</name>
                <description>改訂・編集する</description>
                <requirement>revise_requirement</requirement>
        </item>
        <item>
                <name>delete</name>
                <description>削除・破棄する</description>
                <requirement>delete_requirement</requirement>
        </item>
        <item>
                <name>read</name>
                <description>参照する</description>
                <requirement>read_requirement</requirement>
        </item>
        <item>
                <name>net_delivery</name>
                <description>ネットワークで配布する（送信する）
</description>

        <requirement>net_delivery_requirement</requirement>
        </item>
        <item>
                <name>disc_delivery</name>
                <description>ディスクで配布する（送付する）
</description>

        <requirement>disc_delivery_requirement</requirement>
        </item>
        <item>
                <name>archive</name>
                <description>アーカイブ・バックアップする
</description>
                <requirement>archive_requirement</requirement>
        </item>
</enumeration>
<enumeration>
        <enum_id>emeeting_operation</enum_id>
        <enum_name>E-Meeting Operation</enum_name>
        <description>電子会議システムに関わるオペレーション
</description>
```

【図６】

policy_terminology.xmlのファイルのリストの例を示す図(4)

```
        <item>
                <name>meeting_use</name>
                <description>会議で利用する</description>

        <requirement>meeting_use_requirement</requirement>
        </item>
</enumeration>

<!-- オペレーションごとに適用できる要件の列挙 -->
<!-- ユーザ認証，文書識別，アクセス制御（利用制限）は基本メカニズムとし
て提供されるため，要件には含めない -->
<enumeration>
        <enum_id>hardcopy_requirement</enum_id>
        <enum_name>Hardcopy Requirement</enum_name>
        <description>複写に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description> 監 査 証 跡 の イ メ ー ジ 付 き 記 録
</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>print_requirement</enum_id>
        <enum_name>Print Requirement</enum_name>
        <description>印刷に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description> 監 査 証 跡 の イ メ ー ジ 付 き 記 録
</description>
        </item>
        <item>
                <name>private_access</name>
                <description> プ リ ン ト し た 本 人 に よ る 紙 出 力
</description>
        </item>
```

【図７】

policy_terminology.xmlのファイルのリストの例を示す図（5）

```
        <item>
                <name>trusted_channel</name>
                <description>信頼チャネルの利用（印刷データの暗号化）
</description>
        </item>
        <item>
                <name>embed_trace_info</name>
                <description>プリントアウトに追跡情報埋め込み（透かし，
ラベル，バーコード）</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>fax_send_requirement</enum_id>
        <enum_name>Requirement on Sending Fax
Message</enum_name>
        <description>ファクス送信に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description>監査証跡のイメージ付き記録
</description>
        </item>
        <item>
                <name>destination_restriction</name>
                <description>宛先制限</description>
        </item>
        <item>
                <name>private_mode</name>
                <description>親展モードでの送信</description>
        </item>
        <item>
                <name>trusted_channel</name>
                <description>信頼チャネルの利用（ファクスデータの暗号
化）</description>
        </item>
        <item>
                <name>embed_trace_info</name>
                <description>送信ファクスに追跡情報埋め込み（透かし，ラ
ベル，バーコード）</description>
        </item>
        <item>
                <name>non_repudiation</name>
                <description>否認防止（受取証の取得）</description>
        </item>
```

【図８】

policy_terminology.xmlのファイルのリストの例を示す図(6)

```
</enumeration>
<enumeration>
        <enum_id>fax_receive_requirement</enum_id>
        <enum_name>Requirement      on      Receiving      Fax
Message</enum_name>
        <description>ファクス受信に関わる要件</description>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description> 監 査 証 跡 の イ メ ー ジ 付 き 記 録
</description>
        </item>
        <item>
                <name>private_access</name>
                <description>親展ファクスの宛先本人による取り出し
</description>
        </item>
        <item>
                <name>trusted_timestamp</name>
                <description>信頼タイムスタンプ</description>
        </item>
        <item>
                <name>embed_trace_info</name>
                <description>受信ファクスに追跡情報埋め込み（透かし，ラ
ベル，バーコード）</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>scan_requirement</enum_id>
        <enum_name>Scan Requirement</enum_name>
        <description>スキャンに関わる要件(保存した後については保存要件
を適用する）</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description> 監 査 証 跡 の イ メ ー ジ 付 き 記 録
</description>
        </item>
        <item>
                <name>embed_trace_info</name>
                <description>スキャン画像に追跡情報埋め込み（透かし，ラ
```

【図９】

policy_terminology.xmlのファイルのリストの例を示す図(7)

```
ベル，バーコード) </description>
        </item>
</enumeration>
<enumeration>
        <enum_id>store_requirement</enum_id>
        <enum_name>Store Requirement</enum_name>
        <description>保存に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>encryption</name>
                <description>保存データの暗号化</description>
        </item>
        <item>
                <name>integrity_protection</name>
                <description>保存データの改ざん保護</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>revise_requirement</enum_id>
        <enum_name>Revise Requirement</enum_name>
        <description>改訂に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>versioning</name>
                <description>バージョン管理</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>delete_requirement</enum_id>
        <enum_name>Delete Requirement</enum_name>
        <description>削除・破棄に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
```

【図１０】

policy_terminology.xmlのファイルのリストの例を示す図(8)

```
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description> 監 査 証 跡 の イ メ ー ジ 付 き 記 録
</description>
        </item>
        <item>
                <name>complete_erase</name>
                <description>完全消去</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>read_requirement</enum_id>
        <enum_name>Read Requirement</enum_name>
        <description>参照に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>edit_restriction</name>
                <description> 編 集 禁 止 の デ ー タ の み 参 照 許 可
</description>
        </item>
        <item>
                <name>print_restriction</name>
                <description> 印 刷 禁 止 の デ ー タ の み 参 照 許 可
</description>
        </item>
        <item>
                <name>location_restriction</name>
                <description> 参 照 場 所 限 定 の デ ー タ の み 参 照 許 可
</description>
        </item>
        <item>
                <name>user_restriction</name>
                <description> ユ ー ザ 限 定 の デ ー タ の み 参 照 許 可
</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>net_delivery_requirement</enum_id>
        <enum_name>Delivery via Network Requirement</enum_name>
        <description> ネ ッ ト ワ ー ク 配 信 （ 送 信 ） に 関 わ る 要 件
</description>
        <item>
```

【図１１】

policy_terminology.xmlのファイルのリストの例を示す図(9)

```
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description>監査証跡のイメージ付き記録
</description>
        </item>
        <item>
                <name>trusted_channel</name>
                <description>信頼チャネルの利用（送信データの暗号化）
</description>
        </item>
        <item>
                <name>destination_restriction</name>
                <description>宛先制限（社内のみ配信可能など）
</description>
        </item>
        <item>
                <name>edit_restriction</name>
                <description>編集禁止のデータのみ配信許可
</description>
        </item>
        <item>
                <name>print_restriction</name>
                <description>印刷禁止のデータのみ配信許可
</description>
        </item>
        <item>
                <name>location_restriction</name>
                <description>参照場所限定のデータのみ配信許可
</description>
        </item>
        <item>
                <name>user_restriction</name>
                <description>ユーザ限定のデータのみ配信許可
</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>disc_delivery_requirement</enum_id>
        <enum_name>Delivery via Disc Requirement</enum_name>
        <description>ディスク配布（送付）に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
```

【図１２】

policy_terminology.xmlのファイルのリストの例を示す図（10）

```
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description>監査証跡のイメージ付き記録
</description>
        </item>
        <item>
                <name>encryption</name>
                <description>送付データの暗号化</description>
        </item>
        <item>
                <name>integrity_protection</name>
                <description>送付データの改ざん保護</description>
        </item>
        <item>
                <name>edit_restriction</name>
                <description>編集禁止のデータのみ送付許可
</description>
        </item>
        <item>
                <name>print_restriction</name>
                <description>印刷禁止のデータのみ送付許可
</description>
        </item>
        <item>
                <name>location_restriction</name>
                <description>参照場所限定のデータのみ送付許可
</description>
        </item>
        <item>
                <name>user_restriction</name>
                <description>ユーザ限定のデータのみ送付許可
</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>archive_requirement</enum_id>
        <enum_name>Archive Requirement</enum_name>
        <description>アーカイブ・バックアップに関わる要件
</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
```

【図１３】

policy_terminology.xmlのファイルのリストの例を示す図(11)

```
        <item>
                <name>encryption</name>
                <description>アーカイブデータの暗号化</description>
        </item>
        <item>
                <name>integrity_protection</name>
                <description> アーカイブデータの改ざん保護
</description>
        </item>
</enumeration>
<enumeration>
        <enum_id>meeting_use_requirement</enum_id>
        <enum_name>Meeting-use Requirement</enum_name>
        <description>会議での利用に関わる要件</description>
        <item>
                <name>explicit_authorization</name>
                <description>明示的な許可（利用制限）</description>
        </item>
        <item>
                <name>audit</name>
                <description>監査証跡の記録</description>
        </item>
        <item>
                <name>audit_with_image</name>
                <description> 監査証跡のイメージ付き記録
</description>
        </item>
</enumeration>
</policy_terminology>
```

【図１４】

policy.xmlのファイルのリストの例を示す図（1）

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<about_this_policy>
      <serial_number>RDSP0100-00000000000012-
2023</serial_number>
      <terminology_applied>RDST0100-00000000000001-
9487</terminology_applied>
      <title>Office System Research and Development Center,
DOCUMENT-SECURITY-POLICY</title>
      <version>1.30</version>
      <creation_date>2002/02/18 22:30:24</creation_date>
      <creator>Yoichi Kanai</creator>
      <description>This  is  a  sample  document  security
policy.</description>
</about_this_policy>
<policy>
      <acc_rule>
            <doc_category>ANY</doc_category>
            <doc_security_level>basic</doc_security_level>
            <acl>
                  <ace>
                        <user_category>ANY</user_category>

      <user_security_level>ANY</user_security_level>
                        <operation>
                              <name>hardcopy</name>
                              <allowed/><!--        allowed
without any requirement -->
                        </operation>
                        <operation>
                              <name>print</name>
                              <allowed/><!--        allowed
without any requirement -->
                        </operation>
                        <operation>
                              <name>fax_send</name>

      <requirement>audit</requirement>

     <requirement>explicit_authorization</requirement>
                        </operation>
                        <operation>
                              <name>fax_receive</name>
                              <allowed/><!--        allowed
without any requirement -->
                        </operation>
                        <operation>
                              <name>scan</name>
```

【図１５】

policy.xmlのファイルのリストの例を示す図(2)

```
                                <allowed/><!--          allowed
without any requirement -->
                            </operation>
                            <operation>
                                <name>store</name>
                                <allowed/><!--          allowed
without any requirement -->
                            </operation>
                            <operation>
                                <name>revise</name>
                                <allowed/><!--          allowed
without any requirement -->
                            </operation>
                            <operation>
                                <name>delete</name>
                                <allowed/><!--          allowed
without any requirement -->
                            </operation>
                            <operation>
                                <name>read</name>
                                <allowed/><!--          allowed
without any requirement -->
                            </operation>
                            <operation>
                                <name>net_delivery</name>

        <requirement>audit</requirement>

        <requirement>explicit_authorization</requirement>

        <requirement>print_restriction</requirement>

        <requirement>trusted_channel</requirement>
                            </operation>
                            <operation>
                                <name>disc_delivery</name>

        <requirement>audit</requirement>

        <requirement>explicit_authorization</requirement>

        <requirement>print_restriction</requirement>
                            </operation>
                            <operation>
                                <name>archive</name>
                                <allowed/><!--          allowed
without any requirement -->
                            </operation>
                            <operation>
                                <name>meeting_use</name>
                                <allowed/><!--          allowed
```

【図１６】

policy.xmlのファイルのリストの例を示す図(3)

```
without any requirement -->
                        </operation>
                </ace>
        </acl>
    </acc_rule>
    <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>medium</doc_security_level>
        <acl>
                <ace>
                        <user_category>DOC-
CATEGORY</user_category>

    <user_security_level>ANY</user_security_level>
                        <operation>
                                <name>hardcopy</name>

    <requirement>audit</requirement>

    <requirement>embed_trace_info</requirement>
                        </operation>
                        <operation>
                                <name>print</name>

    <requirement>audit</requirement>

    <requirement>embed_trace_info</requirement>
                        </operation>
                        <operation>
                                <name>fax_send</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>fax_receive</name>
                                <allowed/><!--        allowed
without any requirement -->
                        </operation>
                        <operation>
                                <name>scan</name>

    <requirement>audit</requirement>

    <requirement>embed_trace_info</requirement>
                        </operation>
                        <operation>
                                <name>store</name>
                                <allowed/><!--        allowed
without any requirement -->
                        </operation>
                        <operation>
```

【図１７】

policy.xmlのファイルのリストの例を示す図(4)

```
                                    <name>revise</name>
                                    <allowed/><!--        allowed
without any requirement -->
                              </operation>
                              <operation>
                                    <name>delete</name>
                                    <allowed/><!--        allowed
without any requirement -->
                              </operation>
                              <operation>
                                    <name>read</name>

      <requirement>audit</requirement>

      <requirement>print_restriction</requirement>

      <requirement>location_restriction</requirement>
                              </operation>
                              <operation>
                                    <name>net_delivery</name>

      <requirement>audit</requirement>

      <requirement>explicit_authorization</requirement>

      <requirement>print_restriction</requirement>

      <requirement>trusted_channel</requirement>
                              </operation>
                              <operation>
                                    <name>disc_delivery</name>

      <requirement>audit</requirement>

      <requirement>explicit_authorization</requirement>

      <requirement>print_restriction</requirement>
                              </operation>
                              <operation>
                                    <name>archive</name>
                                    <allowed/><!--        allowed
without any requirement -->
                              </operation>
                              <operation>
                                    <name>meeting_use</name>
                                    <allowed/><!--        allowed
without any requirement -->
                              </operation>
                        </ace>
                        <ace>
                              <user_category>ANY</user_category>
```

【図１８】

policy.xmlのファイルのリストの例を示す図(5)

```
      <user_security_level>ANY</user_security_level>
                        <operation>
                              <name>hardcopy</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>print</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>fax_send</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>fax_receive</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>scan</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>store</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>revise</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>delete</name>
                              <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                              <name>read</name>

      <requirement>explicit_authorization</requirement>

      <requirement>audit</requirement>

      <requirement>print_restriction</requirement>
```

【図１９】

policy.xmlのファイルのリストの例を示す図(6)

```
        <requirement>location_restriction</requirement>
                                </operation>
                                <operation>
                                        <name>net_delivery</name>
                                        <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>
                                <operation>
                                        <name>disc_delivery</name>
                                        <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>
                                <operation>
                                        <name>archive</name>
                                        <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>
                                <operation>
                                        <name>meeting_use</name>
                                        <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>
                        </ace>
                </acl>
        </acc_rule>
        <acc_rule>
                <doc_category>ANY</doc_category>
                <doc_security_level>high</doc_security_level>
                <acl>
                        <ace>
                                <user_category>DOC-
CATEGORY</user_category>

        <user_security_level>ANY</user_security_level>
                                <operation>
                                        <name>hardcopy</name>
                                        <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>
                                <operation>
                                        <name>print</name>

        <requirement>explicit_authorization</requirement>

        <requirement>audit</requirement>

        <requirement>private_access</requirement>

        <requirement>trusted_channel</requirement>

        <requirement>embed_trace_info</requirement>
```

【図２０】

policy.xmlのファイルのリストの例を示す図(7)

```
                        </operation>
                        <operation>
                                <name>fax_send</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>fax_receive</name>
                                <allowed/><!--        allowed
without any requirement -->
                        </operation>
                        <operation>
                                <name>scan</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>store</name>

        <requirement>audit</requirement>

        <requirement>encryption</requirement>

        <requirement>integrity_protection</requirement>
                        </operation>
                        <operation>
                                <name>revise</name>

        <requirement>versioning</requirement>
                        </operation>
                        <operation>
                                <name>delete</name>

        <requirement>complete_erase</requirement>
                        </operation>
                        <operation>
                                <name>read</name>

        <requirement>audit</requirement>

        <requirement>print_restriction</requirement>

        <requirement>location_restriction</requirement>

        <requirement>user_restriction</requirement>
                        </operation>
                        <operation>
                                <name>net_delivery</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
```

【図２１】

policy.xmlのファイルのリストの例を示す図(8)

```
                        <operation>
                                <name>disc_delivery</name>

        <requirement>audit</requirement>

        <requirement>explicit_authorization</requirement>

        <requirement>encryption</requirement>

        <requirement>print_restriction</requirement>
                        </operation>
                        <operation>
                                <name>archive</name>

        <requirement>encryption</requirement>

        <requirement>integrity_protection</requirement>
                        </operation>
                        <operation>
                                <name>meeting_use</name>

        <requirement>explicit_authorization</requirement>
                        </operation>
                </ace>
                <ace>
                        <user_category>ANY</user_category>

        <user_security_level>ANY</user_security_level>
                        <operation>
                                <name>hardcopy</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>print</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>fax_send</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>fax_receive</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>scan</name>
                                <denied/><!-- denied even if
```

【図２２】

policy.xmlのファイルのリストの例を示す図(9)

```
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>store</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>revise</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>delete</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>read</name>

      <requirement>explicit_authorization</requirement>

      <requirement>audit</requirement>

      <requirement>print_restriction</requirement>

      <requirement>location_restriction</requirement>

      <requirement>user_restriction</requirement>
                        </operation>
                        <operation>
                                <name>net_delivery</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>disc_delivery</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>archive</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                        <operation>
                                <name>meeting_use</name>
                                <denied/><!-- denied even if
it is explicitly authorized -->
                        </operation>
                </ace>
```

【図２３】

policy.xmlのファイルのリストの例を示す図（10）

```
            </acl>
        </acc_rule>
</policy>
</document security policy>
```

【図２４】

DSPの識別情報の例を示す図

```
<about_this_policy>
        <serial_number>RDSP0100-00000000000012-2023</serial_number>
        <terminology_applied>RDST0100-00000000000001-
9487</terminology_applied>
        <title>Office System Research and Development Center,
DOCUMENT-SECURITY-POLICY</title>
        <version>1.20</version>
        <creation_date>2002/02/18 22:30:24</creation_date>
        <creator>Yoichi Kanai</creator>
        <description>This is a sample document security
policy.</description>
</about_this_policy>
```

【図２５】

ポリシーの内容を示す一実施例を示す図

```
<policy>
        <acc_rule>
                <doc_category>ANY</doc_category>
                <doc_security_level>medium</doc_security_level>
                <acl>
                        <ace>
                                <user_category>DOC-
CATEGORY</user_category>

        <user_security_level>ANY</user_security_level>
                                <operation>
                                        <name>fax_send</name>
                                        <denied/><!-- denied even if it
is explicitly authorized -->
                                </operation>
                                <operation>
                                        <name>net_delivery</name>

        <requirement>audit</requirement>

        <requirement>explicit_authorization</requirement>
                                        ...
                                </operation>
                                <operation>
                                        <name>fax_receive</name>
                                        <allowed/><!-- allowed without
requirements -->
                                </operation>
                                ...
                        </ace>
                        <ace>
                                ...
                        </ace>
                </acl>
        </acc_rule>
        <acc_rule>
                <doc_category>ANY</doc_category>
                <doc_security_level>high</doc_security_level>
                <acl>
                        ...
                </acl>
        </acc_rule>
</policy>
```

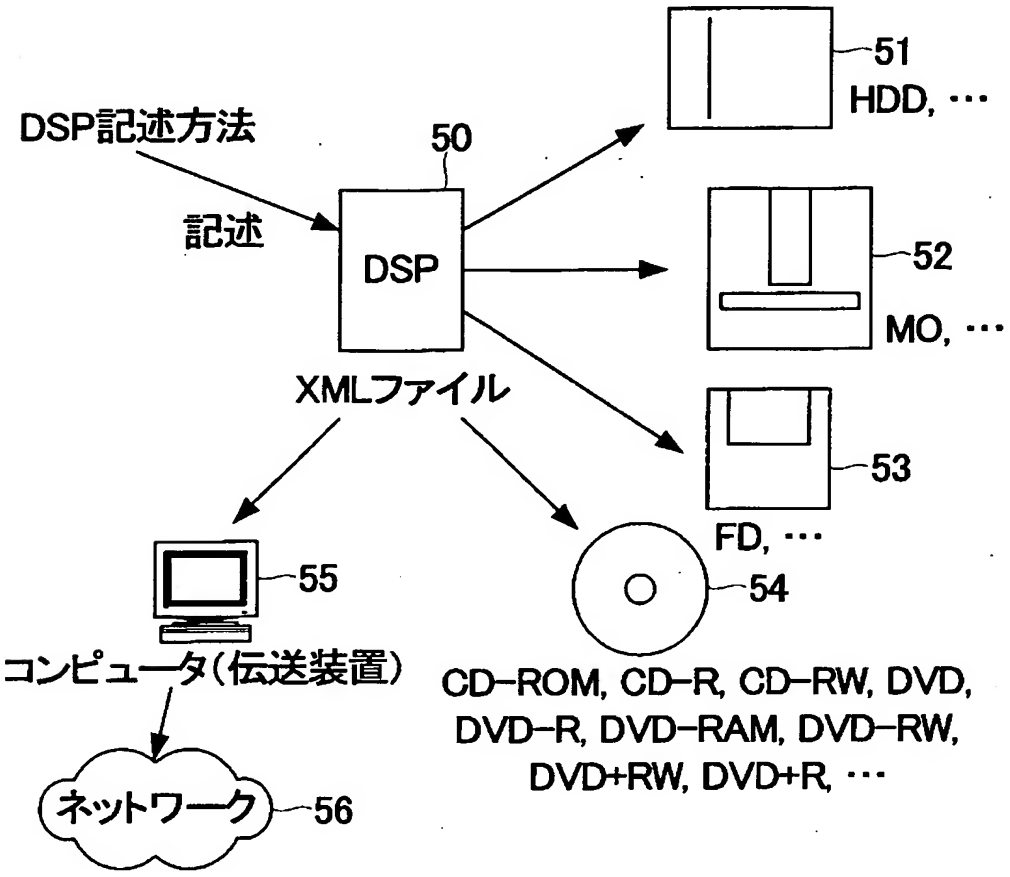
【図２６】

本発明のDSPの別の記述形式の実施例を示す図

```
<policy>
        <acc_rule>
                <doc_category>ANY</doc_category>
                <doc_security_level>medium</doc_security_level>
                <acl>
                        <ace>
                                <user_category>DOC-
CATEGORY</user_category>

        <user_security_level>ANY</user_security_level>
                                <denied_operations> <!-- denied even if
it is explicitly authorized -->
                                        <name>fax_send</name>
                                </denied_operations>
                                <operation>
                                        <name>net_delivery</name>

        <requirement>audit</requirement>

        <requirement>explicit_authorization</requirement>
                                        ...
                                </operation>
                                <operation>
                                        ...
                                </operation>
                                <allowed_operations>    <!--    allowed
without requirements -->
                                        <name>fax_receive</name>
                                        <name>store</name>
                                        ...
                                </allowed_operations>
                        </ace>
                        <ace>
                                ...
                        </ace>
                        ...
                </acl>
        </acc_rule>
        <acc_rule>
                <doc_category>ANY</doc_category>
                <doc_security_level>high</doc_security_level>
                <acl>
                        ...
                </acl>
        </acc_rule>
</policy>
```

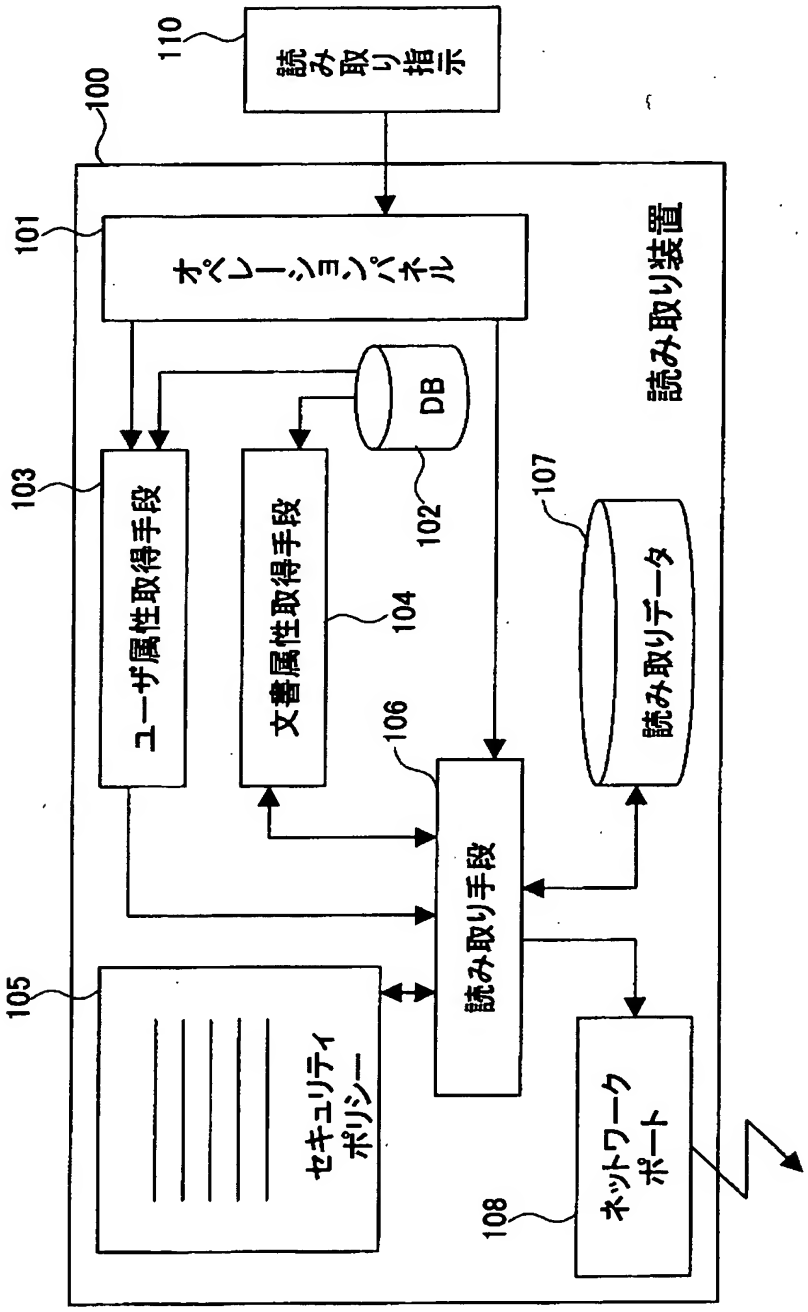
【図２７】

DSPを蓄積し且つ配布する種々の媒体を示す図



【図２８】

本発明の実施例の文書読み取り装置の構成を示す図



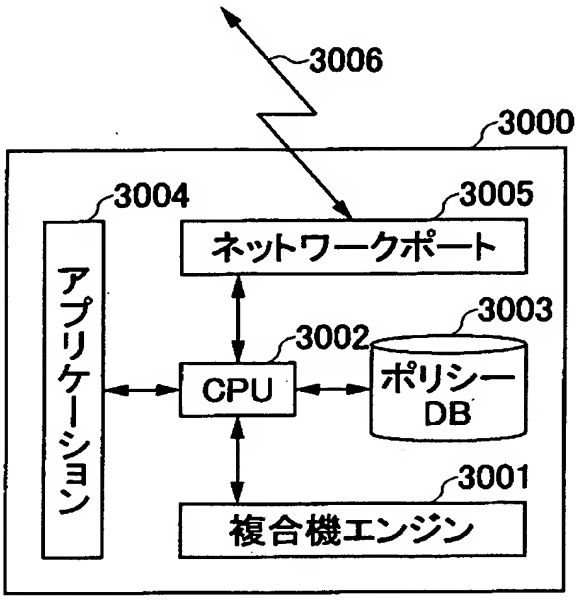
【図２９】

XML(Extensible Markup Language)により記述した本発明の実施例のセキュリティポリシーを示す図

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
          <requirement>print_restriction</requirement>
          <requirement>trusted_channel</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <requirement>audit</requirement>
          <requirement>embed_trace_info</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
</policy>
```

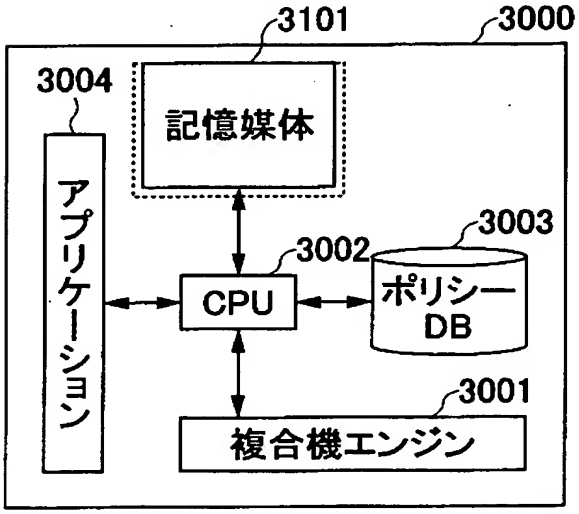
【図３０】

本発明の第3の実施例を示す図



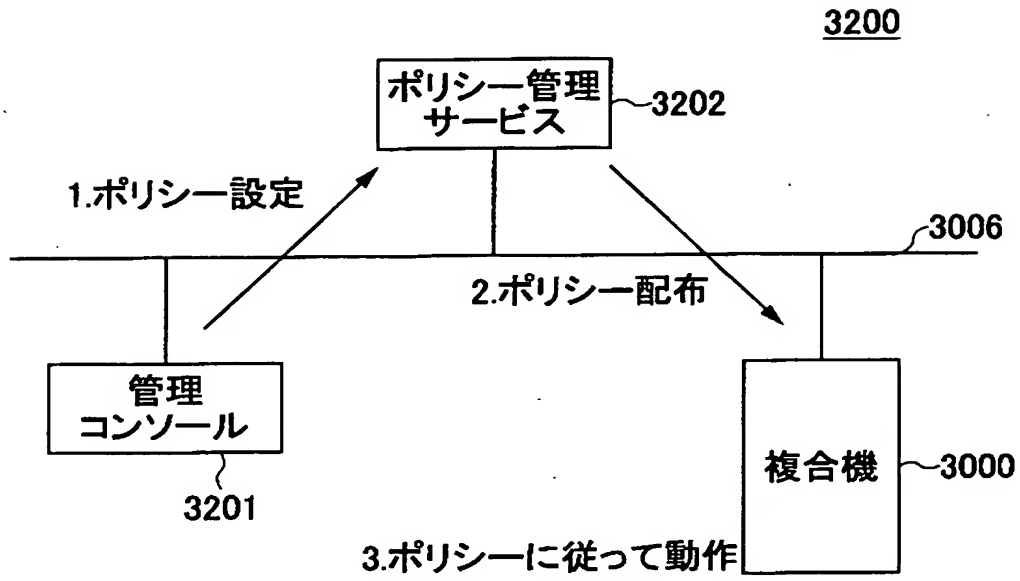
【図３１】

本発明の第4の実施例を示す図



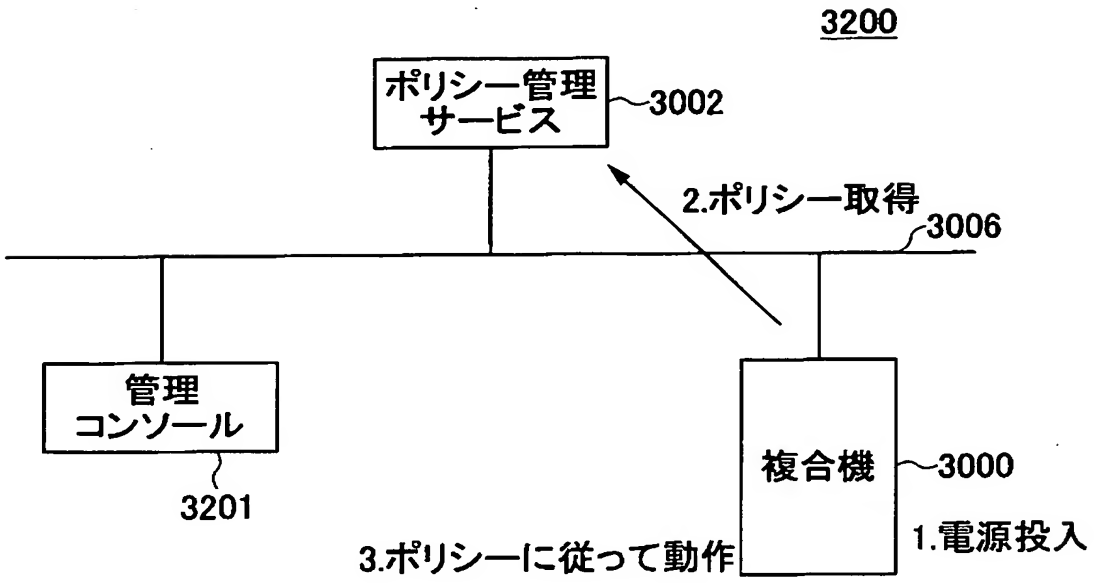
【図３２】

本発明の第5の実施例を示す図



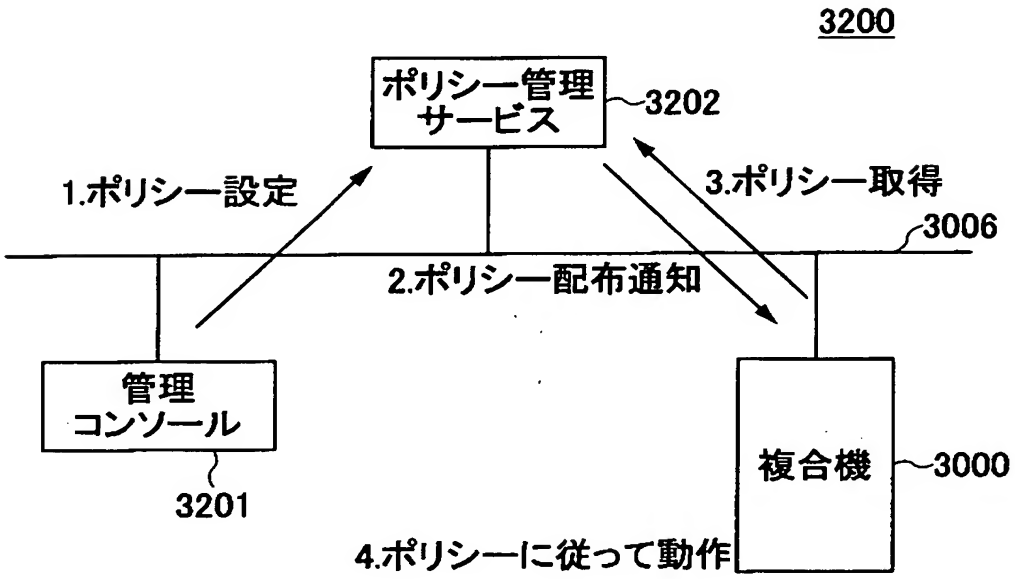
【図３３】

本発明の第6の実施例を示す図



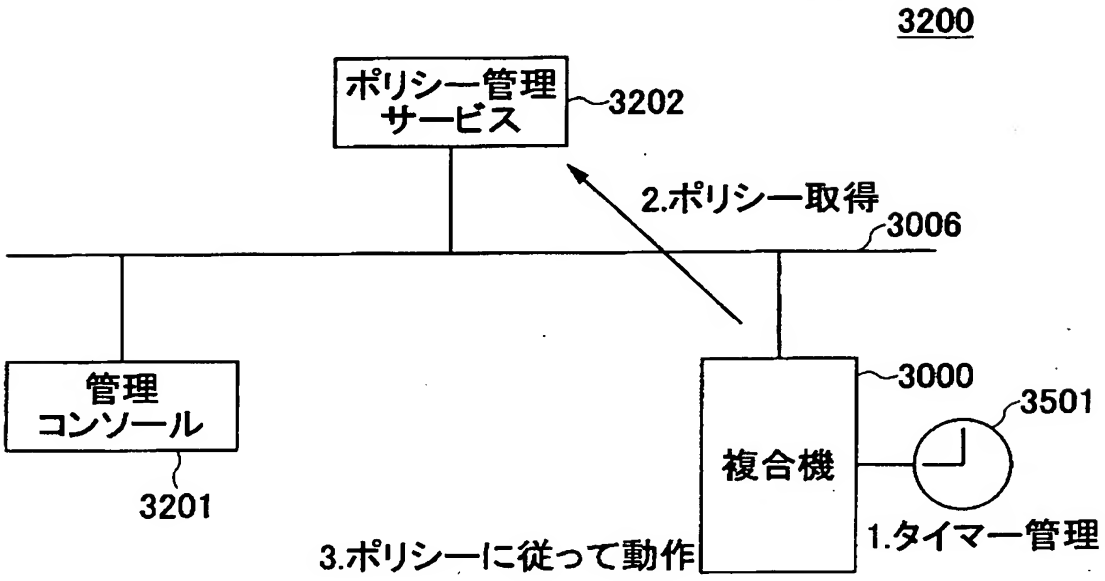
【図３４】

本発明の第7の実施例を示す図



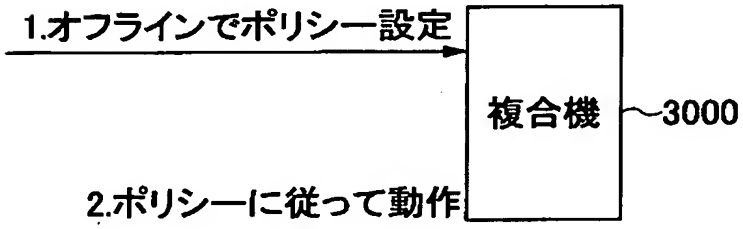
【図３５】

本発明の第8の実施例を示す図



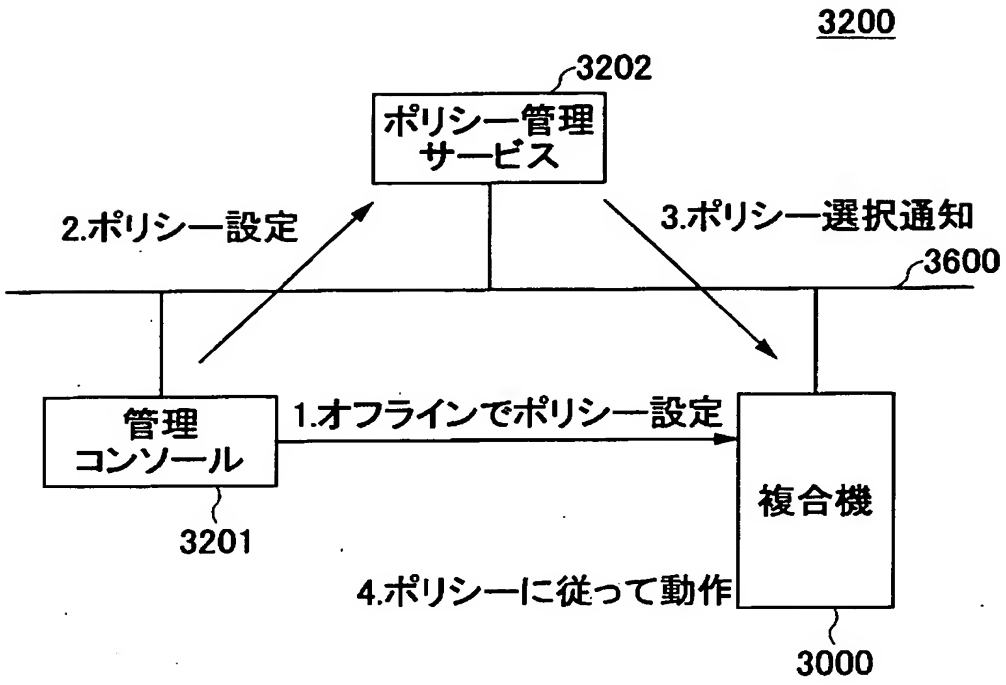
【図３６】

本発明の第9の実施例を示す図



【図３７】

本発明の第10の実施例を示す図



【書類名】　　要約書

【要約】

【課題】　文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法を提供する。

【解決手段】　ユーザ属性を取得し、文書属性を取得し、ユーザ属性と文書属性との組み合わせに対して読み取りが許可されているかをセキュリティポリシーにより判断し、許可されていない場合にはデータを破棄して終了し、許可されている場合には対応する要件をセキュリティポリシーから抽出し、要件がセキュリティポリシー内に存在しない場合には文書の読み取りを行って終了し、要件がセキュリティポリシー内に存在する場合にはすべての要件を読み取る方法で実行可能であるかを判定し、実行可能でない要件が存在する場合にはデータを破棄して終了し、すべての要件を実行可能である場合には抽出された前記要件を満たして文書の読み取りを行って終了する、セキュリティポリシーに基づいて文書を読み取る方法により実現する。

【選択図】　　図１

特願２００２－２９７８８８

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー

２．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー